★GIES- W01 W02 98-558382/48 ★DE 19716111-A1

Mutual authentication method of communicating units - generating random number by first unit which encrypts random numbers generated by first and second units and secrete key only known by first unit with secrete key known by both units for transmission and decryption by second unit

GIESECKE & DEVRIENT GMBH 97.04.17 97DE-1016111
(98.10.22) H04L 9/32, 12/22

The method involves generating a random number by a second unit (B) which is transmitted to first unit (A) which selects a secret key (Ks) only known by the first unit. The first unit encrypts a random number (Za) generated by the first unit using a secrete key (Kab) known by both units. The random number generated by the second unit and the selected secrete key are encrypted as well by the first unit. The result is transmitted as a message (N1) to the second unit which decrypts the received message using the mutual secrete key.

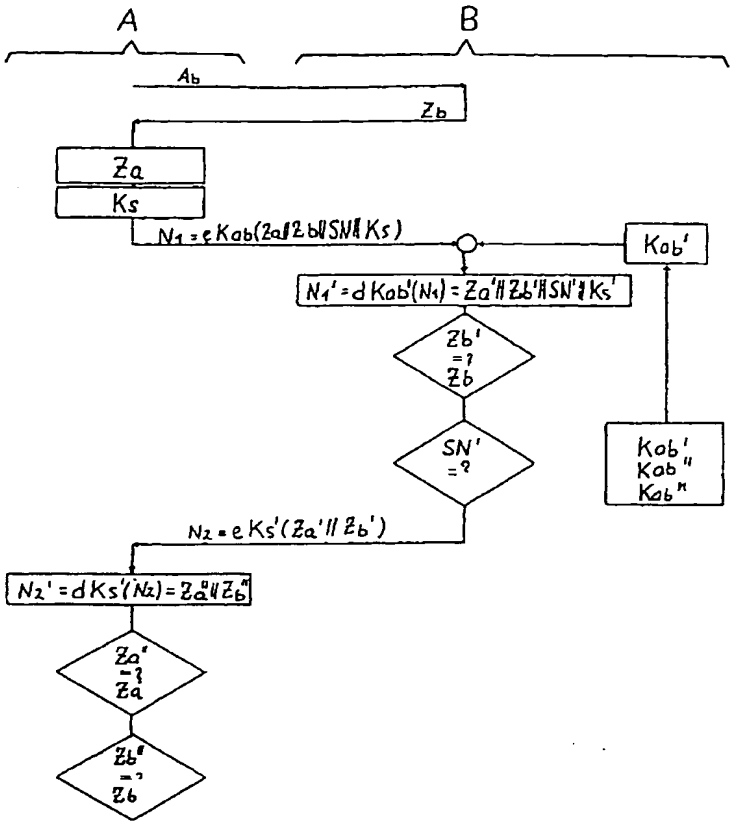
The second unit compares the random number generated by the second unit with the number obtained by decrypting the random number received by the first unit. When the numbers are in conformance the first unit is authenticated by the second unit. The second unit encrypts with the received and decrypted key of the first unit the random number generated by the first unit and transmits the result. The first unit decrypts the received message and compares the generated random number with the number received from the second unit. When the numbers are in conformance the second unit is authenticated by the first unit.

USE - E.g. for chipcard and terminal, mobile radio system.

ADVANTAGE - Prevents appearance of plain text and key during communication and increases security. Enables key exchange during authentication without administration. Allows key to be dynamic and different for each authentication. (4pp Dwg.No.1/1)

N98-435346 W01-A05B W02-C03C

A


A
B
Ab
Zb
Za
Ks
N1 = e Kab (Za // Zb // SN // Ks)
Kab'
N1' = d Kab' (N1) = Za' // Zb' // SN' // Ks'
Zb' =? Zb
SN' =?
Kab' Kab'' Kab'''
N2 = e Ks' (Za' // Zb')
N2' = d Ks' (N2) = Za'' // Zb''
Za' =? Za
Zb'' =? Zb